学校编码：10384　　分类号＿＿＿密级＿＿＿
学号：X2010230633　　UDC ＿＿＿

工　程　硕　士　学　位　论　文

面向信息安全的税务电子申报表单系统的设计与实现

Design and Implementation of Electronic Taxation Reporting Form System Oriented Information Security

许　澄　荣

指导教师姓名：杨律青　副教授
专　业　名　称：　软　件　工　程

论文提交日期：2012　年 10 月
论文答辩时间：2012　年 11 月
学位授予日期：　　年　　月

答辩委员会主席：＿＿＿＿＿
评　　阅　　人：＿＿＿＿＿

2012 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

随着计算机的普及和互联网技术的飞速发展，全国各地税务机关都在致力于网上办税的应用和推广。申报征收、发票开具和认证、抄报税等一系列涉税工作都可以通过网上办税在互联网上得以实现。纳税人可以足不出户完成很多涉税事项的办理，享受着现代信息技术带来的便利。网上申报是网上办税的主要功能。传统的网上申报主要有两种实现模式：表单在线填写的 B/S 模式和离线申报的 C/S 模式。这两种模式在保证数据的安全性、真实性、可靠性方面，在控制服务器并发压力方面以及用户使用体验方面都各自存在一定的不足和缺陷。所以，为了方便纳税人使用，降低服务器并发压力，更为了满足申报数据安全性、真实性、可靠性要求，开发了一个面向信息安全的税务电子申报表单系统。该系统使用 Adobe LiveCycle 技术开发离线模式电子申报表单，同时采用 PKI 技术、CA 认证和数字签名等加密技术确保申报数据的安全和完整。

论文首先介绍了系统的开发背景，分析了国内外有关网上办税应用的发展现状，确定了论文的主要研究方向。其次对项目开发中用到的关键技术进行了简要介绍。然后从宏观方面探讨了系统的目标，从功能性和非功能性两方面分析了系统需要满足的设计需求。随后，论文着重介绍了系统的设计。提出了系统设计的目标和原则，介绍了系统的物理架构和软件架构，划分了功能模块，包括登录模块、申报模块和系统管理模块等三个功能模块，详细介绍了其中申报模块的设计流程，简述了数据库设计，并单独分析了系统的安全性设计。论文在系统实现部分介绍了系统的开发和运行环境，展示了系统的主要界面和关键代码，介绍了系统的运行和测试情况。最后对该系统进行了总结和展望。

关键字：信息安全；PDF 表单；网上申报

Abstract

With the quick popularity of computer and the rapid development of Internet technology, country tax authorities are committed to spread and promote the online tax application. Declaration, tax collection, invoicing issues, tax authentication, transcription, and other series of tax-related jobs can be done on online tax application through Internet. Taxpayers can do a lot of tax-related matters without leaving home, and enjoy the convenience brought by modern information technology. Declaration online is the main function of online Tax application. The traditional online tax declaration has two major realization models: filling forms online called B/S mode and declaring offline by installing client software called C/S mode. These two kinds of modes both have certain deficiencies and defects respectively in ensuring data security, authenticity and reliability, in controlling concurrent pressure of servers and in user experience. So, in order to facilitate the use of taxpayer, reduce server concurrent pressure, also more to meet the requirements of the declaration data security, authenticity and reliability, the electronic taxation reporting forms system has been developed Oriented Information Security. In this system, the Adobe LiveCycle technology is applied to develop the electronic taxation forms reported via offline mode. Meanwhile, the PKI technology, CA authentication, digital signature and the password techniques are used in this system to ensure information security and integrity.

This dissertation firstly introduces the system development background, analyzes the present development situation of the domestic and foreign tax online application, and determines the main directions of the research. Secondly there is a brief introduction on key technologies used in project development. Then the dissertation discusses the goals of the system from the macro aspect, and analyzes the design requirements for the system from the functional and non-functional aspects respectively. Subsequently, the dissertation focuses on the design of system. It not only puts forward the goal and principle of system design, but also introduces the system of physical structure and software architecture, classifies three function modules, including login module, declare module and system management module,

introduces the design process of the declaration module in details, describes the database design, and separately outlines the analysis of system safety design. Regarding the system realization, this dissertation presents the system development and operation environment, demonstrates the main interface and key code, and introduces the running and debugging status of the system. Finally, there are the conclusions and outlook of online tax application system.

Keywords: Information Security; PDF Form; Declare Tax Online

目 录

第一章 绪论 1

1.1 系统开发背景及意义 1

1.2 国内外发展现状 2

1.3 主要研究内容 4

1.4 论文结构安排 4

第二章 系统关键技术 6

2.1 数字签名 6

2.1.1 数字签名的由来 6

2.1.2 数字签名的原理 6

2.1.3 数字签名的分类 7

2.1.4 数字签名的功能 7

2.2 PKI 技术 8

2.2.1 定义 8

2.2.2 组成 8

2.2.3 提供的服务 9

2.2.4 基于 PKI 的安全模型 9

2.3 Adobe LiveCycle 9

2.3.1 PDF 10

2.3.2 定义 10

2.3.3 组件 11

2.4 J2EE 11

2.4.1 体系结构 12

2.4.2 J2EE 核心技术 13

2.5 本章小结 14

第三章　系统需求分析 15

3.1 系统的目标 15

3.2 功能需求分析 16

3.2.1 用户登录 16

3.2.2 申报表下载 16

3.2.3 申报表填写和提交 16

3.2.4 申报结果查询 16

3.3 用户角色分析 16

3.4 用例图 17

3.5 非功能性需求分析 17

3.5.1 安全性 17

3.5.2 真实性 18

3.5.3 可靠性 18

3.5.4 离线方式 18

3.5.5 可操作性 18

3.5.6 可扩展性 18

3.6 本章小结 18

第四章 系统设计 20

4.1 系统设计目标与原则 20

4.1.1 数据的安全性 20

4.1.2 表单填写的离线模式 21

4.1.3 系统的并发性 21

4.1.4 易操作性 21

4.2 系统的架构设计 21

4.2.1 系统的物理架构 22

4.2.1.1 税局宏观的网络拓扑 22

4.2.1.2 系统的网络架构 23

4.2.2 系统软件架构 23
4.3 总体流程图 25
4.4 系统的模块设计 27
4.4.1 功能模块图 27
4.4.2 下载申报表 28
4.4.3 提交申报表 29
4.4.4 结果查询下载 32
4.5 数据库设计 33
4.6 系统安全设计 36
4.6.1 系统面临的安全隐患 36
4.6.2 硬件的安全 37
4.6.3 登录时的 CA 认证 37
4.6.4 表单的数字签名 38
4.6.5 提交表单的加密处理 38
4.7 本章小结 39
第五章 系统实现与测试 40
5.1 系统开发和运行环境 40
5.1.1 开发环境 40
5.1.2 运行环境 41
5.2 主要界面 41
5.2.1 登录界面 41
5.2.2 下载申报表界面 42
5.2.3 提交申报表界面 43
5.2.4 结果查询下载界面 44
5.3 关键代码 45
5.3.1 登录模块 45
5.3.2 下载申报表 45

5.3.3 数字签名 48
5.3.4 提交申报表 49
5.4 系统测试 50
5.4.1 测试环境 51
5.4.2 测试过程 51
5.4.3 测试结果 52
5.5 运行情况 53
5.6 本章小结 53
第六章 总结与展望 54
6.1 总结 54
6.2 展望 55
参考文献 56
致谢 58

Contents

Chapter 1 Introduction 1

1.1 Background and Significance of System Development 1

1.2 Domestic and Foreign Research Profile 2

1.3 Main Research Contents 4

1.4 Framework of Dissertation 4

Chapter 2 Introduction to The Related Technologies 6

2.1 Digital Signature 6

2.1.1 Origin of Digital Signature 6

2.1.2 Principle of Digital Signature 6

2.1.3 Classification of Digital Signature 7

2.1.4 Function of Digital Signature 7

2.2 PKI Technology 8

2.2.1 Definition 8

2.2.2 Components 8

2.2.3 Services 9

2.2.4 Security Model Base on PKI 9

2.3 Adobe LiveCycle 9

2.3.1 PDF 10

2.3.2 Definition 10

2.3.3 Components 11

2.4 J2EE 11

2.4.1 Architecture 12

2.4.2 J2EE Core Technology 13

2.5 Summary 14

Chapter 3 System Analysis 15

3.1 Goal of System Design 15

3.2 Functional Requirements 16

3.2.1 User Login 16

3.2.2 Forms Download 16

3.2.3 Forms Fill Out and Submit 16

3.2.4 Reporting Results Query 16

3.3 Analysis of User Roles 16

3.4 Use Case Diagram 17

3.5 Non-functional Requirements 17

3.5.1 Security 17

3.5.2 Authenticity 18

3.5.3 Reliability 18

3.5.4 Offline Mode 18

3.5.5 Practicality 18

3.5.6 Scalabity 18

3.6 Summary 18

Chapter 4 System Design 20

4.1 Objectives and Principles 20

4.1.1 Data Security 20

4.1.2 Forms Filled In Offline Mode 21

4.1.3 Concurrency of The System 21

4.1.4 Operability 21

4.2 Architecture of The System 21

4.2.1 Physical Architecture 22

4.2.2 Software Architecture of The System 23

4.3 General Flow Chart 25

4.4 Model Design 27

4.4.1 Function Models Figure 27

4.4.2 Forms Download 28

4.4.3 Forms Submit 29

4.4.4 Reporting Results Query and Download 32

4.5 Database Design 33

4.6 Security Design 36

4.6.1 Security Risks 36

4.6.2 Hardware Aspects 37

4.6.3 CA Anthenticate 37

4.6.4 Digital Signature 38

4.6.5 Encryption 38

4.7 Summary 39

Chapter 5 System Implementation 40

5.1 Development and Runtime Environment 40

5.1.1 Development Environment 40

5.1.2 Runtime Environment 41

5.2 Primary Interfaces 41

5.2.1 Login Page 41

5.2.2 Forms Download Page 42

5.2.3 Forms Submit Page 43

5.2.4 Reporting Results Query and Download Page 44

5.3 Key Code 45

5.3.1 Login 45

5.3.2 Forms Download 45

5.3.3 Digital Signature 48

5.3.4 Forms Submit 49

5.4 Debugging 53

5.4.1 Environment 51

5.4.2 Process 51

5.4.3 Result 52

5.5 Running Status of The System 53

5.6 Summary 53

Chapter 6 Conclusions and Future Work 54

6.1 Conclusions 54

6.2 Future Work 55

References 56

Acknowledgements 58

第一章 绪论

1.1 系统开发背景及意义

随着计算机应用的飞速普及和互联网技术的不断发展，目前，我国各地税务机关都在积极开展网上办税服务项目。

网上办税，是一套基于数字证书的用户身份认证技术， 运用现代化的通信手段和计算机及网络信息处理技术，由纳税人通过 Web 方式向税务机关申报应纳税款，税务机关据此征收并扣缴税款的综合税务信息处理系统[1]。通过网上办税系统纳税人可以足不出户完成申报、缴税全流程业务，大大减少了纳税人往返于税务部门的烦恼，也减轻了税局办税大厅的业务压力，节省了大量的人力成本。因此，将更多的税收业务纳入网上办税系统，让纳税人自助完成业务，将是税收信息化的发展方向。

本系统的使用单位从 2006 年起开始推广网上办税，不断拓展其业务功能，已经实现了网上申报、网上认证、网上抄报税、网上出口退税预审、网上发票查验等功能，纳税人通过 CA 认证登录网上办税页面进行各项涉税项目的办理。截至目前，该单位已有 38 项涉税业务可以通过网上办理。全省网上办税注册纳税户达 158 万多户，其中一般纳税人增值税网上申报率达 86%。

广义的网上办税是包括了网上申报、网上认证、网上发票开具及查验等一系列涉税功能的信息处理系统，但是由于申报征收是税收业务最主要且最为关键的业务环节，通常我们可以认为网上申报就指代了网上办税。网上申报是纳税人通过互联网完成申报的过程。申报意味着数据的传递和报表的报送，一般是通过在线填写表单方式，即 B/S 架构模式，或者通过安装客户端软件的离线方式，即 C/S 架构模式来实现的。然而，传统 B/S 架构或 C/S 架构的网上办税系统，越来越多的问题在应用中突显出来。

1、申报数据容易被篡改。在线填写表单，申报数据明文传递，在传递过程中，申报数据很容易被截获并恶意篡改。尽管可以采用 SSL 的加密传输协议来加密申报数据，但这样会明显增加服务器的资源开销，造成服务器负载过大，响应缓慢。

2、申报数据不具有抗抵赖性。不管是 B/S 架构，还是 C/S 架构，多数的网上申报数据都没有经过数字签名。在税务纠纷中，存在纳税人否认申报事实，捏造数据被篡改

的可能，而这时网上办税系统无法提供有说服力的证据。

3、服务器并发压力大。B/S 架构的网上办税系统，大都是遵循同步响应机制，每向服务器发送一次请求，服务器必须马上返回处理结果。随着网上办税的普及，功能的丰富，用户量的增长，系统的业务量将会快速增长。大量在线业务，将使系统不堪重负。

4、用户使用不方便。离线方式的 C/S 架构模式的网上办税，虽然可以有效地缓解服务器的并发压力，但是纳税人需要下载并安装网上申报客户端。对于计算机水平不高的用户来说，安装软件会给他们带来操作上的不便，而且，申报表单格式可能经常变动，客户端的升级维护存在很大的不便。

因此，本文力图探索一种新的方法，在加强数据安全性和抗抵赖性的同时，有效地降低网上办税系统的并发压力，方便用户使用。

1.2 国内外发展现状

信息技术应用于税收领域，极大地提高了税收管理的效率。各国都在不断地拓展网上办税业务，提高其安全性。

美国不断地将新技术应用到税收信息化中。早在上世纪 60 年代，美国已经开始在全国范围内建设税收征管网络，将各项税收业务逐步纳入计算机管理。现在，美国的网上办税业务开展更是引领世界，功能丰富，技术先进，纳税人可以很方便地利用互联网进行税收业务的办理。

澳大利亚也是在全国税务机关中全面运用计算机技术进行各项税收业务的办理。不仅如此，澳大利亚更是实现了税务系统与其他政府机关譬如海关、工商、银行等的网络互联，信息资源充分共享，有效地堵塞了税收漏洞，控制了税源。

不仅是发达国家，很多发展中国家也纷纷致力于网上办税的应用。例如阿尔巴尼亚，规定从 2011 年 2 月 1 日起，企业只能通过网络税务局在线申报纳税，不能再以传统做法通过税务窗口报税，以提高报税透明度，减少企业与税务局直接接触，防止腐败，并降低税务成本，提高申报效率[2]。

在国内，各级税务机关也都纷纷创新思维，充分运用信息技术，拓展网上办税功能。

天津市国税局网上办税快速推进，网上申报、抄税、认证户数比例分别达到